VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

OCHRANA DAT PODNIKU
COMPANY DATA PROTECTION

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — MIROSLAV KOUTNÝ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/2010
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Koutný Miroslav

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Ochrana dat podniku

v anglickém jazyce:

Company Data Protection

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

HANÁČEK, P., STAUDEK, J. Bezpečnost informačních systémů. 1. vyd. Praha: Úřad pro státní informační systém. 2000. 128 s. ISBN 80-238-5400-3.
ARNASON, Sigurjon Thor, WILLETT, Keith D. How to Achive 27001 Certificaiton : An Example of Applied Comliance Management. 1.vydání. London : Auerbach Publications, 2008. 348 s. ISBN 978-0-8493-3648-5.
CALDER, Alan, WATKINS, Steve. IT GOVERNANCE : A Manager's Guide to Data Security and ISO 27001/ISO27002. 1.vydání. London : Kogan Page, 2008. 372 s. 4. ISBN 978-0-7494-5271-1.
BS ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems - Requrements . 1.vydání. London: British Standart Institute, 2005. 44 s.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/2010.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA

V Brně, dne 04.06.2010

ABSTRAKT

Bakalářská práce se zabývá problematikou ochrany dat v podniku. Data jsou jedním z nejcennějších zboží a je nutné, aby měl podnik tato data chráněna. Práce je zaměřena na analýzu současného stavu a navrhuje řešení v souladu s bezpečnostními normami.

KLÍČOVÁ SLOVA

bezpečnost, ISO/IEC 27002, ochrana dat, bezpečnost informačního systému, bezpečnostní pravidla, hrozby, záloha, antivirová ochrana.

ABSTRACT

This bachelor thesis deals with company data protection issue. Company information is the most valuable article therefore it must be protected. The work focuses on analysis of current state and propose solution based on security standards.

KEY WORDS

security, ISO/IEC 27002, data protection, information system security, security rules, threats, backup , anti-virus protection.

BIBLIOGRAFICKÁ CITACE

Koutný, M. *Ochrana dat podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 65 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph. D.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem celou bakalářskou práci zpracoval samostatně, na základě uvedené literatury a pod vedením svého vedoucího bakalářské práce. Prohlašuji, že citace použitých pramenů je úplná, a že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. o právu autorském a o právech souvisejících s právem autorským).

V Brně, 31. Května 2010

Miroslav Koutný

Podpis.....

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Viktoru Ondrákovi, Ph. D. za trpělivost, pozitivní přístup a užitečné rady. Také děkuji Ing. Ivě Frýbortové za konstruktivní připomínky a podporu.

OBSAH

1 Úvod

Bakalářská práce se zabývá problematikou ochrany dat v podniku. Data jsou jedním z nejcennějších zboží a je nutné, aby měl podnik tato data chráněna. V současné době je obecně bezpečnost tématem hodně diskutovaným, nicméně ochrana dat není v českých podnicích dostatečně řešena. V důsledku toho faktoru dochází k úmyslným i neúmyslným únikům dat a podnikům vznikají nemalé škody. Tyto škody mohou mít vliv na ekonomický provoz a existenci podniku.

Úvodní část práce se zaměřuje na konkrétní společnost a popisuje její činnost, organizační strukturu, ekonomickou situaci, ale také její chápání problematiky bezpečnosti informací, popisuje technickou infrastrukturu a analyzuje zde existující metody ochrany dat.

Teoretická část definuje pojem ochrany dat, popisuje metody přístupu k řešení a vymezuje oblasti aplikace ochrany v informačních systémech. Odpovídá také na otázku, jaká data chránit a popisuje vybrané metody ochrany dat.

Poslední část práce je věnovaná aplikaci teoretických poznatků na konkrétní společnost a navrhuje možný postup řešení problematiky ochrany dat v praxi.

2 Vymezení problému a cíle práce

Cílem této práce je na základě analýzy konkrétní firmy zhodnotit její stávající ochranu dat a navrhnout vhodné prostředky ochrany. Jako zdroj čerpání informací je použita dostupná odborná literatura týkající se tohoto tématu a také příslušné technické normy.

3 Analýza současného stavu

3.1 Základní údaje o společnosti

3.1.1 Souhrnné informace

Název společnosti: Svoboda a Syn s.r.o.

Právní forma: společnost s ručením omezeným

Jednatel: František Otřísal, Ing. Karel Svoboda

Společník: Ing. Karel Svoboda

Sídlo: Jahodova 524/62; 620 00 Brno

Provozovna: Sladovnická 20/6, 620 00 Brno

Vývoj: Kraví hora 6, 602 00 Brno

Počet zaměstnanců: 60

3.1.2 Předmět podnikání

Hlavní činností společnosti je výstavba telekomunikačních technologií, stavební a elektro-montážní činnost. Společnost je schopna provádět od jednoduchých činností ve výstavbě, přes montáže a stavby, až po úplná díla na klíč.

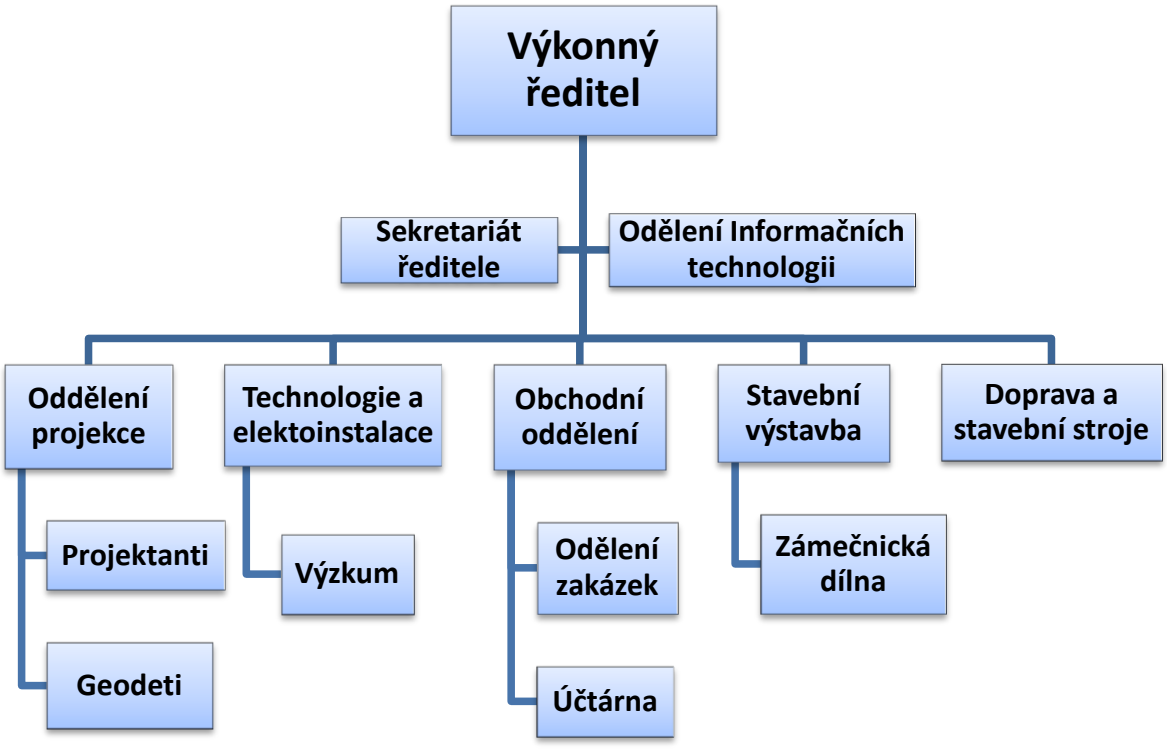
3.1.3 Sortiment služeb

- Zřizování, montáž, údržba a servis telekomunikačních zařízení;
- Výroba, instalace a opravy elektronických zařízení;
- Výroba, instalace a opravy elektrických strojů a přístrojů;
- Výkon zeměměřičských činností;
- Výzkum a vývoj v oblasti přírodních a technických věd;
- Projektování elektrických zařízení;
- Výroba rozvaděčů nízkého napětí a baterií, kabelů a vodičů;
- Montáž, opravy, revize a zkoušky vyhrazených elektrických zařízení;
- Inženýrská činnost;
- Provádění staveb, jejich změn a odstraňování;
- Projektová činnost ve výstavbě.

3.1.4 Oblast trhu

- Společnosti provozující sítě GSM 900, 1800 a 2100, CD MA;
- Společnosti, které získaly licence pro UMTS;
- Podniky poskytující radioreléové sítě SDH, PDH a LMDS;
- Mezinárodní a alternativní telekomunikační operátoři;
- Operátoři poskytující své služby na základě licencí FWA (26 a 3,5 GHz);
- Společnosti plánující výstavbu (inženýrská, projektová a stavební činnost);
- Státní organizace (Ministerstvo obrany, vnitra a spravedlnosti);
- NAMSA – servisní organizace NATO.

3.2 Organizační struktura



Obrázek 1: Organizační struktura společnosti (Zdroj: Vlastní výroba pro potřeby BP)

Popis pracovních pozic

Výkonný ředitel: výkonný ředitel.
Sekretariát ředitele: asistent ředitele, personalista.
Informačních technologie: CIO, vedoucí helpdesku, administrátor, technik.
Projekce: vedoucí projekce, projektant, geodet.
Technologie: vedoucí technolog, technolog, asistentka, skladník, laborant**.**
Obchod: vedoucí, správa zakázek, asistentka, hlavní účetní.
Stavební výstavba: stavby vedoucí, zedníci, kopáči.
Doprava: vedoucí dopravy, dispečer, řidiči.

Chod společnosti je úzce propojen s další společností „Ing. Karel Svoboda“, která zajišťuje prostory provozovny a také IT infrastrukturu.

3.3 Obchodní situace firmy

Na českém trhu firem zabývajících se výstavbou radiotelekomunikačních sítí se pohybuje celá řada subjektů, a to jak co do velikosti obratu, tak i poskytované kvality. Společnosti poskytující výstavbu telekomunikačních sítí často přistupují k neadekvátnímu snižování cen, aby se tak maximálně odlišily od ostatních společností se stejným zaměřením. Již delší dobu dochází k přechodu na takové cenové úrovně, kdy marže neodpovídají nasazení.

Společnost Svoboda a syn, s.r.o. se tedy nachází víceméně v pozici, kdy není schopna ovlivnit cenu směrem nahoru ani dolů. Většina zakázek je získána úspěšným absolvováním veřejné soutěže, ve které je rozhodující nejen cena, ale především termíny, ve kterých je firma schopna zakázky provést a dokončit. Jistou úlohu hraje i to, zda firma již v minulosti spolupracovala se zákazníkem, jaké byly výsledky této spolupráce a jak byl zákazník s prací firmy spokojen.

I když je společnost Svoboda a syn, s.r.o. firmou mladou, je uznávána díky bohatým zkušenostem a dobrým výsledkům jednatele a majitele firmy, pana Ing. Karla Svobody. Řada zakázek je zadávána přímo fyzickou osobou Ing. Karel

Svoboda, která pravidelně vítězí v některých z výběrových řízení. Na Moravě má pak společnost Svoboda a syn, s.r.o. výhodnější pozici, protože je schopna operativnějších reakcí na požadavky zákazníka.

3.3.1 Zákazníci

Nejatraktivnějšími zákazníky jsou velké firmy a velké státní a mezinárodní společnosti. Se vstupem České republiky (tedy i českého průmyslu) do struktur Evropské unie bylo povinností firmy Svoboda a syn, s.r.o. připravit se na „nové konkurenceschopné prostředí", tj. akceptovat a přijmout novou legislativu platnou v zemích EU.

Klíčoví zákazníci

- Telefonica O_2, a.s.;
- Telefonica O_2, a.s. – Slovakia;
- Lukromtel, s.r.o.;
- NAMSA – servisní organizace NATO;
- Vodafone CZ.

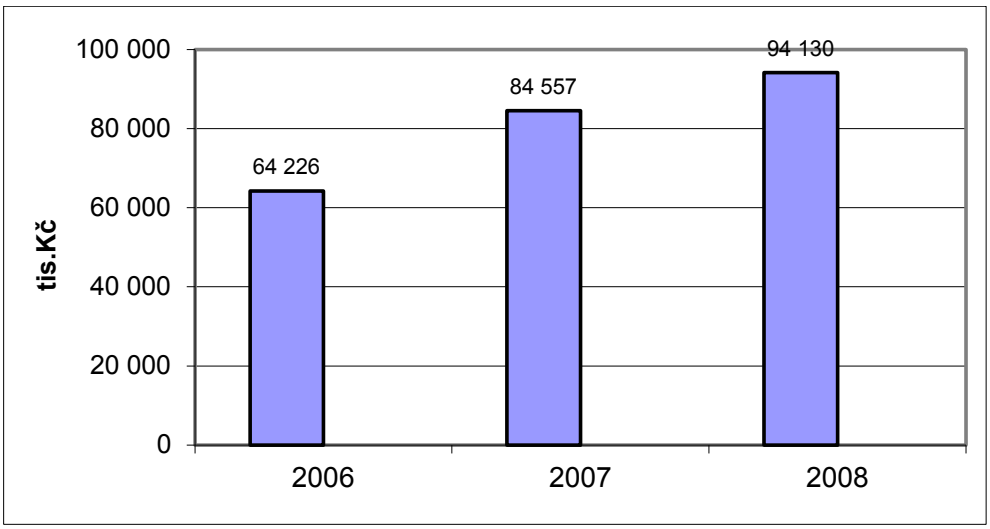
Konkurence

- Lukromtel, s.r.o.;
- Zkrat s.r.o.;
- TECHNISERV IT, spol. s r.o.;
- InfoTel, spol. s r.o.;
- FASO, s.r.o.

Obecně platí, že jednotlivé společnosti mezi sebou úzce spolupracují. Jelikož je nabídka jejich služeb velice podobná, figurují navzájem v roli dodavatelů/subdodavatelů. Rozdílem je pouze cena, za kterou jsou ochotni prodávat, případně akceptace konkrétních podmínek zákazníka.

3.3.2 Vývoj tržeb společnosti

Následující graf zachycuje vývoj tržeb za vlastní výrobky a služby ve společnosti Svoboda a syn, s.r.o. za roky 2006 až 2008. Z grafu je patrné, že tržby společnosti rok od roku stoupají, což lze vnímat jako pozitivní faktor. V roce 2007 byl nárůst tržeb oproti roku 2006 navýšen o 24% a o rok později o dalších 11%. Informace z roku 2009 nebyly společností poskytnuty.



Obrázek 2: Vývoj tržeb společnosti (Zdroj: Materiály firmy Svoboda a syn)

3.4 Popis infrastruktury

3.4.1 Klientská část

Software:

Každý počítač obsahuje základní kolekci programů, které jsou společné pro všechna oddělení:

- Adobe Acrobat;
- Ultra VNC;
- Mozilla Firefox;
- Internet Explorer 8;
- Windows XP.

Specializovaný Software:

- Autocad - oddělení projekce;
- RTS – obchodní oddělení;
- Microstation, Groma,Geobáze – oddělení geodetů;
- MS Office 2003/2007 – kancelářský balík programů;
- Dispatcher – Sledování dopravní techniky.

Hardware:

- Uživatelské stanice: Dell Optiplex;
- Notebooky: Dell Latitude.

Přehled:

- Celkem pracovních stanic: **50 ks**;
- Celkem notebooků: **20 ks**.

3.4.2 Serverová část

Software

- Windows 2003, 2008, 2008R2 Server;
- CentOS Linux;
- FreeBSD;
- Mail Server: Merak Mail Server – IMAP;
- Virtualizace: VMware Esxi 4.0.

Hardware

- Dell Power Edge 2850;
- Dell Power Edge 1950;
- Diskové pole Dell MD 3000;
- Dell Power Edge 6650;
- Dell Powe Edge 2800;
- Zálohovací mechanika LTO 2.

Přehled

Rozložení serverů a počty (ks):

- Fyzické servery: **7**;
- Virtuální servery: **12**;
- Celkem produkční servery: **16**.

Role serverů a počty (ks):

- Aplikační server: 7;
- Doménový kontrolér: 4;
- Terminal Server: 1;
- Mail Server: 1;
- File Server: 2;
- Backup Server: 1.

3.4.3 Síťové prostředí

Hlavní síťový prvek Dell Power Connect 6248 a 2x Dell Power Connect 6224 tvoří dohromady 108mi portový L2/L3 switch. Servery jsou připojeny rychlostí 1 Gbit. Diskové pole rychlostí 4 Gbit. Pro návštěvníky je k dispozici Wifi, separovaná od hlavní datové sítě. Pobočky jsou připojeny pomocí Wifi technologie 5,4 Ghz na vzdálenost 3,5 km. Jednotlivé vzdálenější budovy jsou připojeny optickou technologií 100 Mbit.

3.4.4 Data společnosti

Umístění

Servery

Centrální úložiště tvoří diskové pole MD 3000, které má pro uživatele kapacitu 1,5 TB. Zbylá část 500 GB se využívá pro zálohy produkčních serverů. Z historických důvodů je k dispozici původní file server s kapacitou 200 GB, ten se v současné době nepoužívá.

Stanice

Pro uložení se používá výhradně centrální datové pole. Uživatelé si vytvářejí pracovní kopie částí dat. Výsledky své práce ukládají zpět na centrální úložiště.

Struktura dat

Vzhledem k historickému vývoji prošla struktura uložených dat několika přeměnami. V důsledku toho vznikla neuspořádaná struktura adresářů a souborů, ve které se mnoho dat opakuje. Tvoří veliké množství nepřesně pojmenovaných souborů v nepřehledné hierarchii adresářů.

Velikosti dat a jejich nárůst

Aktuální velikost dat je 600 GB. Většina (80%) je tvořena daty, která se již nemění. Denní nárůst nových dat se pohybuje kolem 100 MB.

Význam dat pro společnost

Společnost si neuvědomuje cenu vlastních dat a jejich význam. To dokladuje fakt, že záloha dat nebyla vůbec řešena. Největší cenu pro společnost mají existující smlouvy a dokumentace staveb. Stejně tak fotodokumentace základních stanic.

Ochrana dat

Společnost využívá RAID 5 pole v rámci centrálního úložiště a také doménový koš. Jedná se o funkci file serveru, kde smazaný soubor na síťovém disku není po smazání uživatelem smazán, ale uložen do doménového koše, takže data jsou k dispozici až do úplného vymazání správcem. Zpravidla do jednoho roku zpět. Jedná se však pouze o smazané soubory.

Řízení přístupu k datům

Mimo přístupu k ekonomickým datům, není přístup k datům nijak řízen.

3.4.5 Archivace a zálohování

Tato oblast není ve společnosti řešena. Vlastní ale potřebný hardware. Backup server s LTO2 mechanikou a 4 TB diskového prostoru. NAS s kapacitou 3 TB. Tyto

servery nejsou v současné době využity. Aplikační servery se zálohují automaticky do vyhrazené oblasti centrálního diskového pole.

Vedení společnosti požaduje rychlou obnovu dat. Důraz je kladen hlavně na hlavní diskové pole, kde jsou uloženy zejména ekonomické informace, fotodokumentace a technické dokumentace.

3.4.6 Antivirová ochrana

V současné době společnost nedisponuje komplexním řešením antivirové ochrany. Antivirus je nainstalován na noteboocích společnosti a jedné pracovní stanici. Na serverech antivirus není, s výjimkou mail serveru, který má integrovaný antivirus v Merak Mail Serveru.

3.4.7 Přenos dat s okolím

Je omezen pouze na e-mailovou komunikaci. Mezi pobočkami probíhá sdílení souborů v rámci vnitřní sítě izolované od sítě internet. Využívají se také výměnná media (CD/DVD, Flash disky).

3.4.8 Informační systém

Ekonomický informační systém:

Společnost využívá systém Pohoda od společnosti Stormware.

Dílčí informační systémy:

Oddělení technologie používá systém vyvinutý technologií PHP pro evidenci výjezdních zásahů. Oddělení dopravy využívá systém Dispatcher pro sledování polohy vozidel společnosti a evidenci pohonných hmot.

Společnost v současné době vyvíjí vlastní informační systém. Cílem je propojit jednotlivé prvky do funkčního celku za účelem vytvoření komplexního informačního systému. Také se jedná o nasazení Groupware od společnosti IceWarp.

Řízení přístupu k aplikacím

Přístup k aplikacím není systematicky řízen, je orientován na jednotlivé uživatele, nikoliv skupiny. Existují také aplikace, které mají volný přístup, např. IS oddělení technologie.

3.5 Bezpečnostní povědomí společnosti

Bezpečnost je vnímána specifickým způsobem. Vzhledem ke spoluprácí se servisní organizací NATO, má společnost bezpečnostní prověrku na stupeň tajné. Důsledkem toho existuje v zabezpečené místnosti výpočetní technika, která splňuje nároky definované dle zákona o utajovaných skutečnostech. Komplexní vnímání bezpečnosti však chybí. Je zde náznak o fyzickou bezpečnost ve formě průmyslových kamer a čipů pro chráněný přistup. To vše bez dalších návazností.

3.6 Shrnutí nedostatků současného stavu

- Nedostatečná antivirová ochrana;
- Chaoticky uspořádána data;
- Žádné metody zálohování;
- Společnost nezná cenu vlastních dat;
- Neřízený přístup k datům a aplikacím.

4 Teoretická východiska

4.1 Data

4.1.1 Definice pojmu data

Data jsou statická fakta, která jsou časově nezávislá a vhodná pro další zpracovávání [8].

Data jsou vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat [7].

Data lze také chápat jako vytváření poznatků ve formě, která je v hodná pro další zpracování [7].

Objektivně, sledovatelné vyjádření skutečností nebo znalosti na nějakém mediu tak, že je lze předávat [8].

4.1.2 Význam dat pro společnost

V současnosti patří data společnosti mezi její nejcennější komoditu; jedná se o nehmotný majetek uchovávaný v elektronické formě. Ztráta dat může tedy negativně ohrozit fungování a v krajním případě i zánik společnosti.

4.1.3 Hodnota dat

Hodnota dat je dána:

- vynaloženými náklady na jejich pořízení a údržbu;
- cenou danou informačním obsahem, užitnou hodnotou.

Způsob stanovení ceny dat zahrnuje hledisko věcné a časové [8]. Metody ocenění dat jsou detailně rozepsány v kapitole 4.3.9 Ocenění aktiv.

4.1.4 Prostředí ochrany dat

Informační systém

Informační systém lze chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují. Procesy rozumíme funkce, které zpracovávají informace do systému vstupujících a transformujících je na informace ze systému vystupujících.

Dle normy ISO 23821 je Informační systém definován jako systém zpracování informací spolu s návaznými organizačními prostředky (personálem), technickými a funkčními prostředky. Takový systém získává a distribuuje informace [8].

Datový zdroj

Jedná se o organizovaný výskyt dat, který podléhá řádu informačního systému. Data jsou uložena převážně v databázích, které mou být separátní, dle charakteru systému [2]. Tato data jsou významná pro celou společnost.

Informační technologie

Veškerá technika, která se zabývá zpracováním informací, tj. zejména výpočetní, komunikační technika, ale i její programové vybavení.

Datový zdroj

Úložiště jedinců, kteří tato data využívají pouze pro vlastní potřebu. Jedná se o nahodilý výskyt dat, která jsou uložena v blíže nespecifikované hierarchii adresářů a názvů souborů. Jsou to např. lokální kopie části souboru informačního systému nebo unikátní data uložená na sdílených sítových discích, lokálních úložištích či výměnných mediích. Význam těchto dat je omezen pouze na vlastníka těchto dat.

4.1.5 Důvod ochrany dat

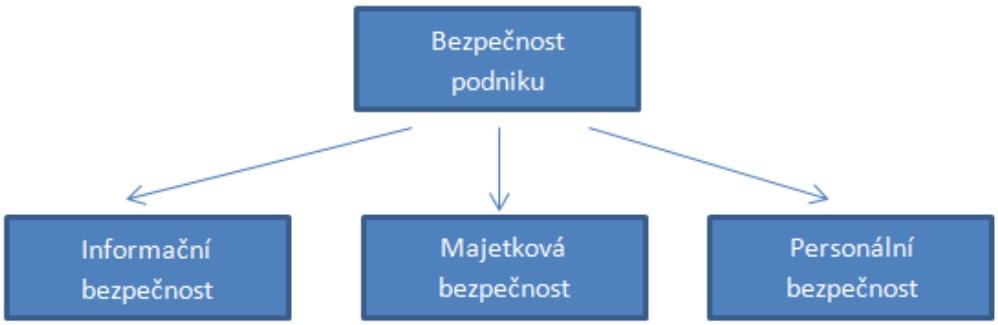
- Vlastní zájem vázaný na význam dat pro podnik. Utajení důvěrných informací podniku, zamezení jejich zneužití, zajištění jejich dostupnosti a celistvosti.
- Smlouva a závazky - jedná se o závazky organizace vůči spolupracujícím externím společnostem a klientům, vyplývající z podmínek uzavřených smluv a dohod.

- Zákonné povinnosti

  - Zákon č. 21/1992 Sb., o bankách ve znění pozdějších předpisů;
  - Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů;
  - Zákon č. 227/2000 Sb., o elektronickém podpisu;
  - Zákon č. 148/1998 Sb., o utajovaných skutečnostech;
  - Zákon č. 97/1974 Sb., o archivnictví [11].

4.2 Bezpečnost podniku

Bezpečnost podniku lze rozdělit na 3 specifické oblasti viz Obrázek 3.



Obrázek 3: Struktura bezpečnosti podniku (Upraveno dle: [3])

Tato práce se zabývá pouze jednou podmnožinou bezpečnosti, ale v případě systémového přístupu řešení bezpečnosti je třeba zohlednit všechny oblasti.

4.3 Informační bezpečnost

Norma ISO/IEC 17799 definuje pojem informační bezpečnosti jako ochranu informací před celou škálou hrozeb tak, aby byl zajištěn chod organizace, minimalizovány škody, maximalizována návratnost investic spolu s obchodními příležitostmi.

Literatura [1] definuje informační bezpečnost jako systém ochrany dat a informací během vstupu, zpracování, ukládání, přenosu a likvidace prostřednictvím logických, fyzických, technických, programových a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity, a dostupnosti těchto hodnot.

Základem kvalitní informační bezpečnosti je pořádek a také komplexnost. Bez nich bude jakákoliv snaha o dosažení kvalitního zajištění informačního systému předem odsouzena k nezdaru [12].

4.3.1 Cíle informační bezpečnosti

Cílem informační bezpečnosti je zachování těchto atributů:

- Důvěrnost – zajištění, že informace je přístupná pouze těm, kteří k ní mají mít přístup.
- Dostupnost – informace je na požádání autorizovaným uživatelům vždy dostupná.
- Integrita – existence mechanizmu zajišťujícího celistvost a neměnnost informace.

Obecně je informační bezpečnost chápána jako možnost přístupu autorizovaných osob v rozsahu a tehdy, kdy je to potřebné [3]. Absolutní bezpečnost neexistuje a nutně tedy vždy existuje míra akceptovatelného rizika. Pohled na bezpečnost pak bude odlišný ve státním sektoru (armáda, policie) a v komerčních sektorech, stejně tak závisí na typu organizace a její velikosti.

4.3.2 Charakteristika pojmů

Aktivum (Asset) – všechny hmotné a nehmotné statky, vše co má pro uživatele Informačního systému jistou hodnotu. Za nejcennější leze považovat peníze, majetek, data a informace, jejichž zneužití, ztráta nebo modifikace, které by společnosti způsobily určitou škodu.

Bezpečnost (Security) - vlastnost nějakého objektu nebo subjektu, která definuje míru ochrany proti možným škodám a hrozbám.

Hrozba (Thread) – skutečnost, událost, síla nebo osoba, jejíž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost.

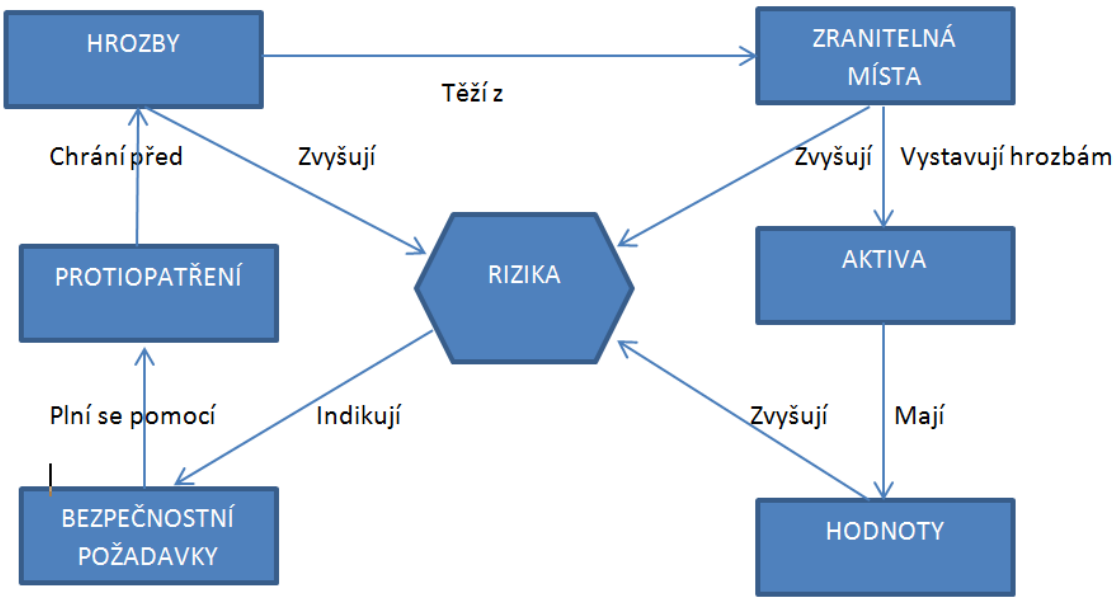
Riziko (Risk) - pravděpodobnost, s jakou bude hodnota aktiva zničena nebo poškozena působením konkrétní hrozby. Jedná se o míru ohrožení aktiva.

Ocenění rizik (Risk Assesment) - proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, jemuž je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby se snížila pravděpodobnost vzniku škody na přijatelnou úroveň [15].

Zranitelnost (Vunerability) - nedostatek nebo slabina bezpečnostního systému, která muže být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiva. Každé aktivum je zranitelné, protože jeho hodnotu ohrožují různé vlivy.

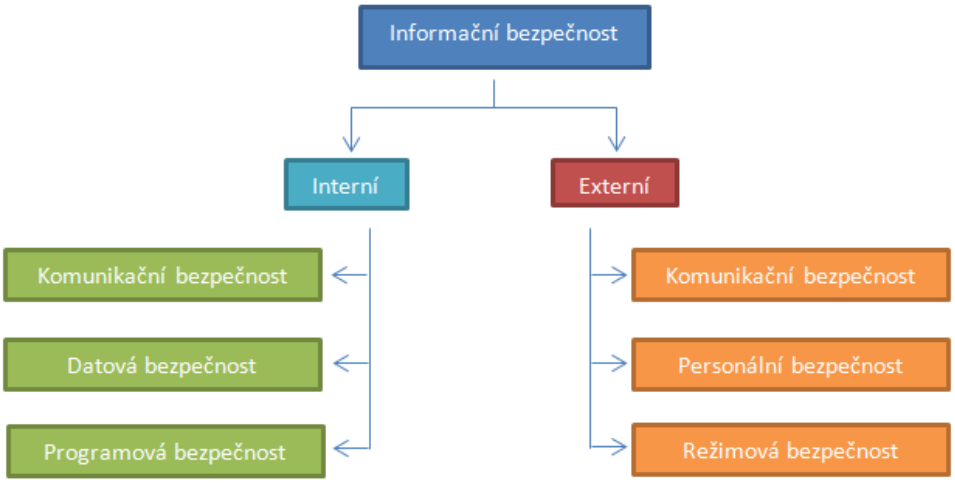
Útok (Attack) - bezpečnostní incident, úmyslné využití zranitelného místa ke způsobení škod/ztráta aktiva Informačního systému, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech [9].

4.3.3 Vztah pojmů informační bezpečnosti



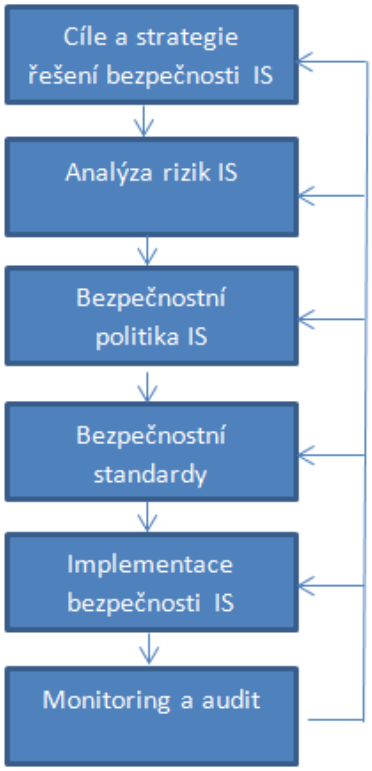
Obrázek 4: Vztah pojmů informační bezpečnosti (Upraveno dle [3])

4.3.4 Kategorizace informační bezpečnosti



Obrázek 5: Rozdělení informační bezpečnosti (Upraveno dle [3])

4.3.5 Schéma systémového řešení informační bezpečnosti



Obrázek 6: Schéma systémové přístupu řešení informační bezpečnosti (Upraveno dle [6])

4.3.6 Bezpečnostní cíle

Rozhodnutí, co bude hlavním cílem a jaká cesta k němu povede.

Bezpečnostní cíl by měl obsahovat:

- Zhodnocení současné úrovně informační bezpečnosti.
- Definice principů řízení a požadované úrovně informační bezpečnosti.
- Navržení postupu k dosažení požadované úrovně informační bezpečnosti [7].

4.3.7 Analýza rizik

Přístupy k analýze rizik

Základní přístup k analýze rizik

Základní přístup spočívá v zavedení určité sady bezpečnostních opatření bez podrobnější analýzy (např. dle doporučení některých bezpečnostních norem). Lze realizovat rychle, nevýhodou je neznalost míry rizik a tudíž možná neadekvátnost bezpečnostních opatření.

Neformální analýza rizik

Tento přístup není založen na definovaných metodologiích, ale vychází ze zkušeností jednotlivců a znalosti prostředí informačního systému. Úroveň míry rizik je obvykle určována kvalifikovaným odhadem odborníka v oblasti analýzy rizik (často je využito účelových interview s pracovníky společnosti).

Tyto metody jsou časově nenáročné, často přináší problémy při zvládání rizik aplikováním bezpečnostních opatření vzhledem k jejich finančním nákladům (neznáme hodnotu aktiv, nevíme, zdali budou finance účelně vynaloženy). Obtížnější obhájení závěrů analýzy rizik před managementem. Příkladem neformální analýzy rizik je Microsoft Security Assetment Tool.

Podrobná analýza rizik

Jsou založeny na matematickém výpočtu míry rizik. Tyto metody umožňují aplikovat přiměřená bezpečnostní opatření vzhledem k ceně chráněných aktiv. Nevýhodou je pracnost a časová náročnost metod. Příkladem těchto metodik analýzy rizik informačních systémů jsou metodiky CRAMM a COBRA (vyvinuta ve Velké Británii společností C&A) V obou případech se jedná o metodiku, kterou lze využít pomocí SW nástroje.

Kombinovaný přístup

Kombinace předchozích metod [11].

Nástroj Microsoft Security Assetment Tool

Nástroj je navržen tak, aby identifikoval rizika organizace a poskytl zhodnocení těchto rizik týkajících se technologie, procesu, a lidských zdrojů organizace. Vychází z norem ISO/IEC 17799 a NIST-800.x. Bezpečnostní hodnocení se skládá z 200 otázek, které jsou rozděleny do 4 kategorií:

- Infrastruktura;
- Aplikace;
- Operativa;
- Lidské zdroje.

4.3.8 Identifikace aktiv

Identifikace spočívá ve vytvoření seznamu aktiv, která leží uvnitř hranice analýzy rizik. Bude se tedy jednat o následující aktiva:

a) Informace – databáze, sestavy dat, dokumenty;

b) HW – servery, pracovní stanice, směrovače, tiskárny, kabely;

c) SW – operační systémy, aplikační programy;

d) Budovy a místnosti, v nichž se aktiva typu a) až c) fyzicky nacházejí [9].

4.3.9 Ocenění aktiv

Při provádění analýzy rizik potřebujeme znát odhad ceny (významu, důležitosti) jednotlivých aktiv ležících uvnitř hranice analýzy rizik. Stanovení ceny fyzických aktiv je jednoduchá – na základě pořizovací ceny odpovídajícího zařízení.

Obtížněji se stanovuje cena datových aktiv – obvykle se stanovuje na základě odhadu velikosti škody, kterou by společnosti způsobilo vyzrazení a zneužití dat, jejich neoprávněná modifikace, nedostupnost a případné zničení (princip odhadu „Co by se stalo, kdyby …?“. Hodnota je pro tato aktiva odvozována nepřímo přes soustavu nepeněžních měřítek.

Doporučuje se vzít v úvahu alespoň následující nepeněžní parametry a z nich vyplývající ztráty:

• Nedodržení legislativy nebo předpisů;
• Zhoršení výkonu činnosti společnosti;
• Porušení obchodního tajemství;
• Finanční ztráty, přerušení aktivit činnosti společnosti;
• Zhoršení bezpečnosti prostředí [11].

4.3.10 Klasifikace dat

Je to nutnost v době, kdy se informační systémy organizace stále více napojují na systémy třetích stran. Rozděluje informace do různých skupin z hlediska jejich kritičnosti pro společnost. To následně umožní implementovat bezpečnostní kontrolní mechanizmy ve vazbě na tuto kritičnost a důležitost. Pro účely účinného provedení klasifikace informací je důležité odpovídající personální zajištění a stanovení odpovědností.

Rozdělení podle **typu přirazených práv**:

- Uživatelé
- Operátoři
- Administrátoři

3 klíčové skupiny uživatelů:

- Vlastníci informací
- Správci informací
- Uživatelé informací

Vlastníci

Jde o manažery mimo oblasti IT, kteří jsou zodpovědní za daný typ nebo skupinu informací. Jsou to také ti manažeři, kteří jsou zodpovědní za tvorbu těchto informací a kteří by byli ztrátou nejvíce postiženi. O klasifikaci a ceny dat rozhoduje především její vlastník.

Správce informací

Vlastníci informací nemají zdroje ani zkušenosti nutné pro správu informací, a proto delegují některé aktivity potřebné ke správě informací na jiné zaměstnance. Např. zaměstnanec z oddělení IT, který přiděluje podle potřeb příslušná práva pro manipulaci s těmito daty, provádí zálohování a stará se o celkovou správu těchto cenných informací.

Uživatel informace

Je to zaměstnanec organizace, třetí strany nebo jiná osoba, autorizovaná pro využívání informací ke svým pracovním povinnostem. Vedení společnosti rozhoduje o klasifikace informací a řeší případné spory v klasifikaci.

Zásady klasifikace

- Vlastník informací by neměl být z oblasti IT;
- Nutná podpora nejvyššího vedení;
- Vlastníci informací by měli mít pravomoci zakotvené v bezpečnostní politice tak, aby klasifikaci a odpovídací kontroly mohli uplatňovat a vynucovat [3].

4.3.11 Bezpečnostní politika

Základní dokument odpovídající na otázky:

- CO chránit?
- PROČ to chránit?
- JAK chránit?
- JAK to ověřit?
- CO dělat v případě havárie?

Základní dokument pro řešení informační bezpečnosti organizace. Vytváří závazky pro celou společnost a definuje východiska pro všechny další aktivity organizace v oblasti informační bezpečnosti.

Hlavním cíle bezpečnostní politiky:

- Definovat hlavní cíle při ochraně informací;
- Stanovit jak řešit bezpečnost;
- Určit pracovníky a zodpovědnosti.

Plnění bezpečnostní politiky musí být vynutitelné, jinak nemá smysl, a aplikuje se na všechny pracovníky organizace [2].

4.3.12 Bezpečnostní struktura organizace

Součástí bezpečnostní politiky je také stanovení rolí v souladu s organizační strukturou organizace. Jedná se o generické role, které jsou přiřazovány již existujícím rolím organizační struktury.

Řídicí výbor bezpečnosti

- Schvalování bezpečnostní politiky organizace;
- Strategické rozhodování;
- Propojení s managementem organizace.

Fórum bezpečnosti IT

- Řeší interdisciplinární problémy a schvaluje směrnice;
- Monitoruje implementaci programu bezpečnosti IT celé společnosti;
- Doporučuje potřebné zdroje;
- Hodnotí účinnost bezpečnostní politik.

Bezpečnostní manažer

- Dohled nad implementací programu bezpečnosti IT;
- Aktualizace politiky bezpečnosti a bezpečnostních směrnic;
- Koordinace přezkoumávání incidentů.

Bezpečnostní správce

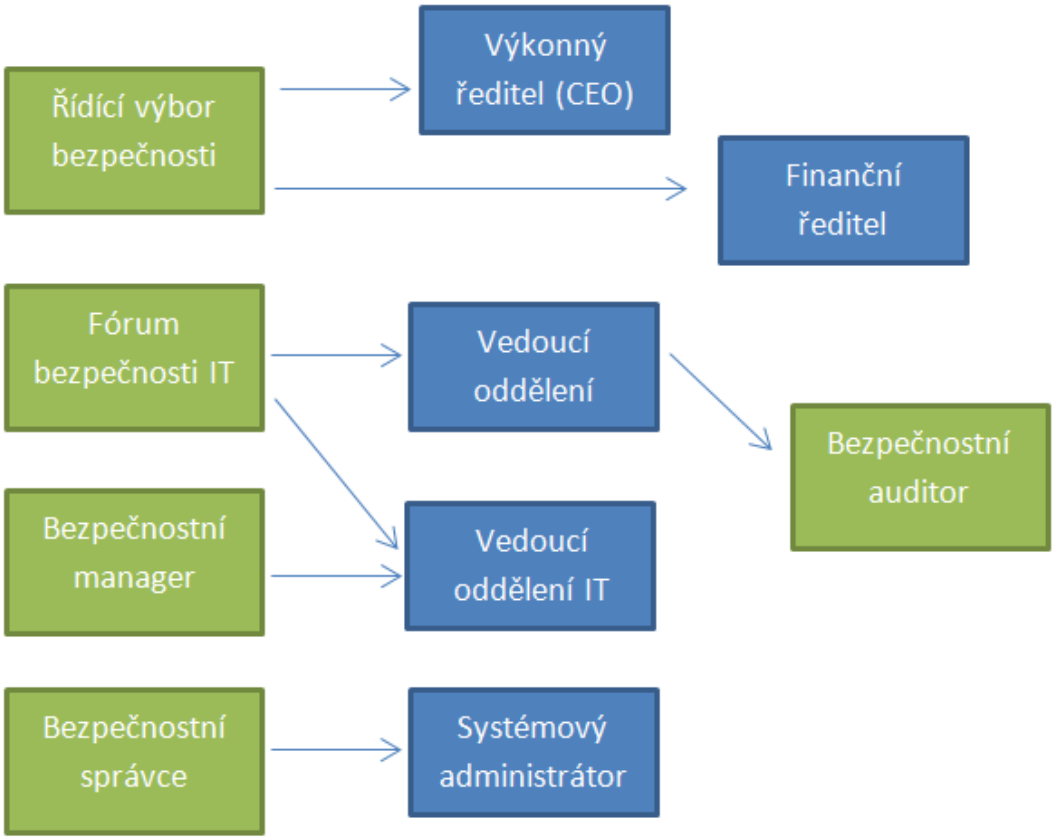
- Výkonný bezpečnostní orgán;
- Vývoj a implementace plánu bezpečnosti;
- Monitorování implementace a používání ochranných opatření IT;
- Může být sdružený s rolí systémového administrátora.

Bezpečnostní auditor

- Kontrolní orgán.

Malé a střední organizace obvykle volí jednoho pracovníka bezpečnosti pro celou společnost, jeho zodpovědnosti pak odpovídají všem popisovaným rolím. Pokud to organizace umožňuje, je vhodné tyto role rozdělit, aby nenastala vysoká koncentrace pravomocí jednotlivce [6].

Následující obrázek ukazuje možné propojení organizační struktury a bezpečnostních rolí.



Obrázek 7: Příklad propojení organizační struktury a bezpečnostních rolí (Zdroj: Vyrobeno pro potřeby BP)

4.4 Ochrana dat

Možnosti ochrany dat podniku

Literatura [3] stejně jako dostupné normy [15] popisuji metody ochrany dat a jeho výsledkem je soubor opatření a postupů.

Obrázek 8: Struktura ochrany dat podniku (Zdroj: Vyrobeno pro potřeby BP)

4.5 Organizační opatření

Toto opatření je realizováno formou vnitropodnikových nařízení a směrnic, které musejí zahrnovat celou činnost informačního systému, řešení krizových stavů a zásady personální bezpečnosti. Těmito směrnicemi musí být jasně vymezena a delegována zodpovědnost každého pracovníka za konkrétní věc. Tato opatření se vydávají písemně [3].

Příklady opatření:

- Zásady a pravidla pro práci s výpočetní technikou v rámci organizace;
- Určení stupně důvěrnosti a ochrany jednotlivých informací;
- Definice bezpečnostních zón a pravidla řízení přístupů;
- Postupy pro jednotlivá oddělení při příchodu a odchodu nového zaměstnance.

4.6 Fyzická opatření

Jsou to všechna opatření použitá k zajištění fyzické ochrany informačního systému proti náhodným a úmyslným hrozbám. Zajišťují ochranu IS pomocí technických prostředků ochrany. Fyzická opatření ale řeší také bezpečné uložení datových nosičů. Dále také způsoby likvidace již nepotřebných informací a médií, ochrany proti požárům, zajištění dodávky stabilizovaného zdroje elektrické energie [3].

4.7 Technická opatření

Zabývají se kvalitním výběrem a nasazením technických prostředků do informačního systému, zajištění jeho včasného kvalitního servisu tak, aby nenarušil požadovanou dostupnost zdrojů. Součástí je také ochrana technických prostředků před elektromagnetickým vyzařováním. Příkladem je služba HP Carepack od společnosti Hewlett-Packard a Dell Support od společnosti Dell [3].

4.8 Zálohování

Cíl

Zajistit vhodné technologie zálohy a obnovy vycházející z potřeb organizace a udržovat integritu a dostupnost informací a prostředků pro jejich zpracovaní. Tyto postupy shrnout v politice zálohování.

Aplikační scénář

Rozhodující je analýza zálohovaných dat, tj. množství zálohovaných souborů a také charakter adresářové struktury. Tvorba záloh by měla být řešena systematicky a respektovat zejména potřeby uživatelů - vlastníků rozhodujících o citlivosti a požadavcích na obnovitelnost dat, kteří by si měli být vědomi důležitosti zálohování pro svou práci, nikoliv být založena pouze na úvahách, znalostech a zkušenostech zaměstnanců útvaru informatiky [3].

Pří vytváření zálohovacího scénáře je třeba zohlednit následující podmínky:

- Stanovení minimálního nutného množství záloh;
- Rozsah vytváření záloh a frekvence, s jakou budou vytvářeny, by měla odpovídat struktuře dat organizace;
- Obnovovací procesy by měly být pravidelně testovány, aby byla prověřena jejich účinnost;
- U kritických systémů by zálohování mělo zahrnovat veškeré systémové informace, aplikace;
- Definování rolí a zodpovědností v rámci politiky zálohování [16].

Způsob ověření stávajícího stavu

Existence zálohovacího zařízení, existence politiky zálohovaní, které pokrývají potřeby organizace, záloha potřebných dat.

4.8.1 Zálohovací schémata

D2D (Disc-to-Disc): Zálohování z disku na disk

Výhoda: Rychlá záloha.

Nevýhoda: Není k dispozici více kopií, nelze udělat offsite backup.

D2T (Disc-to-Tape): Zálohování z disku na pásku

Výhoda: Více kopií záloh, lze je uložit mimo podnik off-site backup.

Nevýhoda: Nutný kontinuální datový tok při zálohování, jinak hrozí poškození zálohovací pásky.

D2D2T (Disc-to-disc-to-tape): Zálohování z disku na disk a poté na pásku

Kombinace předchozích schémat.

4.8.2 Zálohovací metody

Úplná záloha

Při každé operaci se zálohuji všechna data. Důsledkem toho je vytížená infrastruktura, neboť je přenášena celková velikost zálohovaných dat.

Inkrementální záloha

Zálohují se kopie těch souborů, které se změnily od poslední inkrementální zálohy (resp. od úplné zálohy, v případě první inkrementální zálohy). Obnova dat zahrnuje několik kroků, nejdříve obnovení úplné zálohy a pak postupně jednotlivé inkrementy, než se dosáhne požadovaného bodu obnovení.

Rozdílová záloha

Zálohují se kopie jen těch souborů, které se změnily od poslední úplné zálohy. Obnova dat zahrnuje obnovení úplné zálohy a patřičnou rozdílovou zálohu.

Virtual Full Backup

Po provedení počáteční replikace zdrojových dat dochází k uložení jednotlivých rozdílů změn. Změny se ukládají podle synchronizačního intervalu. Obnova dat je možná zpětně, a to dopočítáním rozdílu od stavu současného a zálohovaného [14].

4.8.3 Umístění záložních medií

Onsite backup

Záložní kopie jsou umístěny na jednom místě např. serverovna, kancelář správce.

Offsite backup

Záložní kopie jsou umístěny na více místech. Např. týdenní záloha je pravidelně odvážena mimo areál společnosti do bezpečnostní schránky [2].

4.8.4 Způsob přístupu k datům

Souborový

Popis:

Jedná se tradiční způsob zálohování ze souborového systém. Pro zálohu je vždy použít soubor spolu s uložením cesty kde se nachází a také další atributy.

Výhody:

Univerzálně použitelné.

Nevýhody:

V případě většího množství souborů a násobné hierarchii adresářů dochází k zahlcení systému a spotřebě systémových prostředků zálohovacího serveru. Dochází k ohromným časovým prodlevám. Proces přípravy zálohování je tedy časově náročný a v některých případech i neproveditelný [13].

Blokový

Popis:

Blokový způsob zápisu obchází souborový systém a čte data přímo z disku nebo svazku. To umožňuje nový způsob zálohování. Odpadá pak problém fragmentovaných souborů a také problém násobných adresářů a počtů souborů.

Výhody:

Minimální časová náročnost zálohování a obnovy. Podpora funkce snímkovaní s časovou známkou. Tedy lze získat několik verzí souboru zpětně.

Nevýhody:

Podporuje pouze některé operační systémy. Nutnost pořízení kapacitně většího úložiště pro vytvoření záložního obrazu [14].

4.8.5 Kategorie zálohovacích programů:

Klasické

Záloha je prováděna na souborovém systému s využitím zálohovacích metod a schémat na medium. Záloha je prováděna dle pevně daných časových schémat.

Změny jsou indikovány pomocí atributů souborů a kontrolních součtů. Obnova dat je záležitostí hodin [13].

Online záloha

Stejně jako klasická metoda zálohy dat je prováděna na souborovém systému. Změny souboru jsou vypočteny metodou výpočtu kontrolních součtu. Záloha je prováděna online.

Kontinuální záloha dat

Zálohování se provádí na základě změny datových bloků na klientských discích (nekontrolují se soubory či adresáře). Okamžitá obnova dat při jakékoliv ztrátě (obnova souborů, adresářů, disků či celých operačních systémů) [14].

Porovnání

Tabulka 1: Porovnání kategorii zálohovacích programů (Upraveno dle [14])

	Klasická záloha	Online záloha	Kontinualní záloha dat
Metoda zálohování	Plná/Přírůstková/Rozdílová	Plná/Přírůstková	Plná virtuální
Časový rámec ztracených dat při pohromě	Dny	Dny	**Minuty**
Metoda výpočtu rozdílu	Atributy/Kontrolní součty	Kontrolní součty	Průniky rozdílů přírůstků
Velikost zálohovací okna	Hodiny/Dny	Hodiny/Dny	**Minuty**
Online zálohování	NE	**ANO**	**ANO**
Kritická cesta zálohovaciho okna	Čas načtení soupisu souborů pro zálohu	Čas načtení soupisu souborů pro zálohu	**Čas načtení rozdílu od poslední zálohy**

4.8.6 Dodavatelé řešení

IBM Tivoli Storage Manager FastBack/Disaster Recovery

- Zástupce kontinuální ochrany dat.
- Cena: 45 000,- Kč a vyšší.
- Stručný popis: Moderní řešení pro rychlé a spolehlivé zálohování firemních dat. Důraz je kladen na efektivní a rychlé zálohování změn datových bloků na klientském disku. Klíčovou vlastností je okamžitá obnova dat po kritickém výpadku nebo havárii (soubory, adresáře, celé disky nebo operační systémy).

Symantec Backup Exec

- Zástupce klasické ochrany dat
- Cena: 20 000,- Kč a vyšší.
- Stručný popis: Navržen pro rostoucí potřeby současných podniků a přináší komplexní diskovou a páskovou ochranu, a obnovení dat pro prostředí Windows. Zálohování a obnovení s certifikací společnosti Microsoft pro úplné portfolio produktů Windows Server 2008.

4.9 Antivirová opatření

Cíl

Zvolit vhodný produkt pro ochranu integrity programového vybaveni a dat. Podmínkou je také společná centrální administrace všech instalovaných antivirových produktů.

Aplikační scénář

Řešení by mělo být řízeno pomocí centralizované správy a mělo by podporovat všechny instalované antivirové produkty. Dále je nutné zajištění pravidelné distribuce aktualizace jak na stanice/servery, tak na notebooky. Mimo toho je třeba zvyšovat bezpečnostní povědomí uživatelů formou školení, či zasíláním informačních emailů.

Způsob ověření stávajícího stavu

Ověření zda stanice/server obsahuje antivirový software a také zda je spravován centrálně.

4.9.1 Moduly antivirových řešení:

Antivirus

Součásti antivirového programu jsou obvykle následující komponenty:

Rezidentní štít (On-Access scanner)

Rezidentní štít zcela automaticky a neustále vyhledává viry v datech (nejčastěji v souborech), se kterými přichází uživatel do styku a může tak testovat:

- Spouštěné soubory / programy;
- Otevírané (kopírované) soubory;
- Ukládané soubory;
- Systémové oblasti.

Hledat viry ve spouštěných souborech je pro rezidentní štít nutným. Z principu je zřejmé, že skener provede antivirovou kontrolu souboru ještě před okamžikem, než dojde k jeho spuštění.

Kontrola e-mailu (Mail Protection)

Kontrola e-mailu je řešena pomocí integrace do poštovního klienta, popřípadě se kontroluje datové spojení, což je nezávislé na použitém poštovním klientovi.

On Demand Scanner

On-demand skener je takový, který vyhledává viry (skenuje) až po vydání požadavku uživatelem (proto „on-demand“ – „na vyžádání“). Požadavek je často vydáván manuálně, obvykle vybráním požadované oblasti pro test (adresáře, pevný disk, disketa atd.) [5].

Anti-spyware

Odstraňuje programy typu spyware. Spyware využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Jsou odcizována pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí.

Desktop firewall

Firewall slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje.

Centrální správa

Jedna se o centralizované řešeni, tj. existuje jeden centrální bod, ze kterého je správa řízena. Zajišťuje distribuci programových a datových komponent antivirovému programu. Lze také monitorovat stav, provádět vzdálenou obsluhu a vykonávat tak požadované testy či manuální aktualizace virové báze.

4.9.2 Hodnocení antivirových programů:

Pravděpodobně nejuznávanější srovnávací testy publikuje anglický časopis Virus Bulletin (www.virusbtn.com). Dochází k nim obvykle každé dva měsíce a použitá cílová platforma je neustále měněna. Díky tomu lze v průběhu roku narazit na testy pod Windows NT, Linux, Windows XP, Novell atd. Antivirovým systémům, kterým se podaří detekovat 100% ITW (In the Wild) virů v obou kategoriích (on-access i on-demand) a zároveň projít na „Clean Files Test Set“ bez falešného poplachu je uděleno ocenění „Virus Bulletin 100% Award” [10].

4.9.3 Dodavatelé řešení:

ESET Smart Security Business Edition

Součásti řešení:

- Anti-Spam;
- Anti-virus;
- Anti-spyware;
- Desktop firewall;
- Remote Administrator.

Cena:

- 750 Kč bez DPH stanice/server.

McAfee Total Protection for Endpoint Essentials

Součásti řešení:

- Anti-virus;
- Anti-spyware;
- Desktop firewall;
- Site blocking;
- Desktop host intrusion preventiv;
- Onsite Management Epo.

Cena:

- 1450 Kč bez DPH stanice/server.

McAfee VirusScan for Linux Servers

Součásti řešení:

- Anti-virus

Cena:

- 2300 Kč bez DPH

ESET NOD32 File Security pro Linux

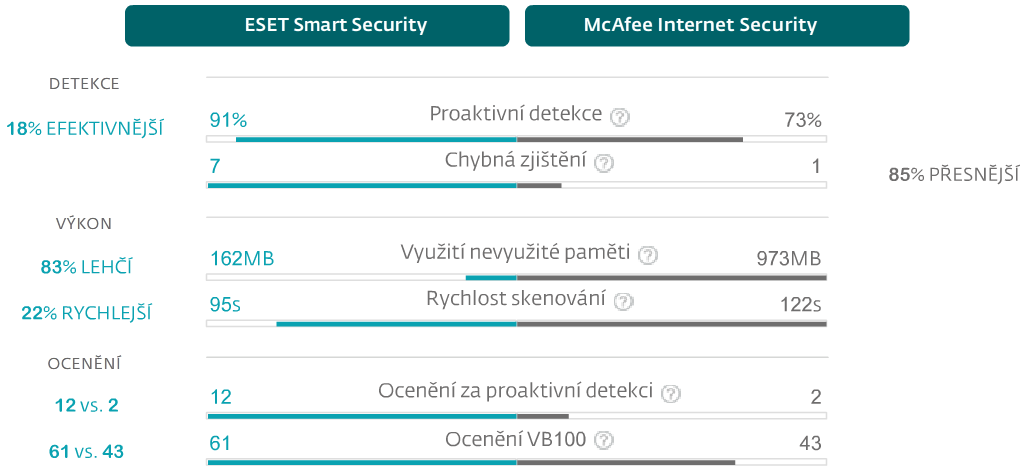
Součásti řešení:

- Anti-viru

Cena:

- 3400 Kč bez DPH

4.9.4 Porovnání dodavatelů řešení



Obrázek 9: Porovnání vybraných antivirových programů (Převzato z: [10])

4.10 Šifrování

Kryptografická opatření

Techniky pro utajení obsahu dat a informací tak, aby byly zabezpečeny při ukládání a přenosu. Využití metody šifrování pro obsah komunikace, dat v souborech, např. digitální podpisy [4].

4.11 Programová opatření

Umožňují chránit informace přímo v počítačích pomocí programových bezpečnostních prostředků.

- Kontrola přístupu

  Zabraňuje neoprávněným uživatelům v práci s informacemi, k nimž nemají povolen přístup. Základním způsobem realizace je přístupové heslo.

- Monitorování činnosti

  Slouží ke sledování a zaznamenávání podezřelých aktivit uživatelů.

- Hlášení

  Systém reportů, zpráv oznamující významnou událost.

4.11.1 Kontrola přístupu

Cíl

Řídit přístup k informacím, předcházet neoprávněnému přístupu k informacím uložených v počítačových systémech.

Aplikační scénář

Přístup k prostředkům pro zpracování informací by měl být řízen na základě provozních a bezpečnostních požadavků. Pro omezení přístupu k aplikačním systémům by měly být použity bezpečnostní prostředky. Logický přístup by tedy měl být omezen na oprávněné uživatele. Systém by měl kontrolovat přístup k datům a funkcím aplikačního systému v souladu s politikou přístupu.

Způsob ověření stávajícího stavu

Ověření, zda jsou na aktuálních datových zdrojích aplikovány mechanizmy ověření uživatelů. Zjištění, zda aplikace je dostupná jenom úzkému spektru uživatelů.

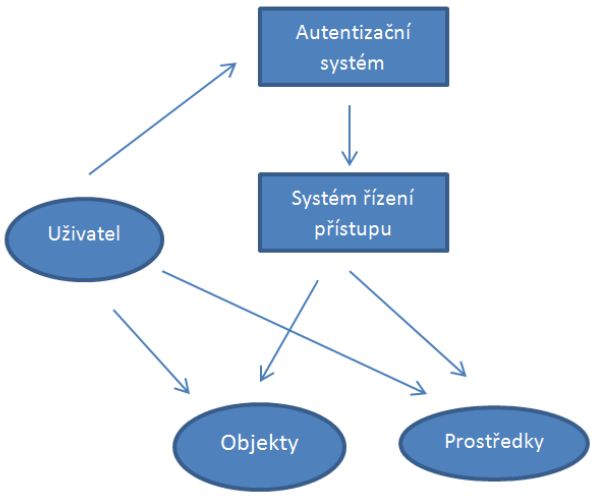
4.11.2 Popis řízení přístupu

Předpokladem správného řízení přístupu je:

- Technické opatření – existence omezení na úrovni (čtení, zápis, vymazání, spuštění).
- Organizační opatření – uživatelé rozdělení do skupin, které vychází z organizační struktury [9].

4.11.3 Technické opatření

Schéma řízení přístupu k objektům



Obrázek 10: Řízení přístupu ke zdrojům a objektům systému (Upraveno dle [5])

Nepovinné řízení přístupu

Jedná se o řízení přístupu, kde každý uživatel má přiřazená jistá práva k jednotlivým objektům. Systém pak hlídá, zda uživatel, který přistupuje k objektu, má dostatečné oprávnění k dané činnosti. Tato pověření jsou pak uložena v Access Control Listu – ACL. Tyto ACL jsou aplikované na jednotlivé adresáře či soubory. Technická implementace ACL je pak rozdílná jak v systémech běžících na technologii MS Windows nebo Linux.

Implementace přístupu

Pro přístup k datům je vhodné definovat skupiny se zkratkou Res_Objekt_Pravo („Res“ - Resource neboli zdroj). Tyto skupiny lze definovat v adresářové struktuře, kterou společnost používá.

Příklad:

Res_Ucto_Write: skupina, která bude k adresáři Ucto přiřazovat uživatele s právem zápisu.

Pro aplikace je vhodné využívat přístupových skupin se zkratkou ACN_Aplikace.

Příklad:

Acn_Pohoda, skupina pro uživatele programu Pohoda. Členové této skupiny mají právo spustit program Ekonomického systému Pohoda.

Podle typu operačního systému je provedena vazba na aplikace a chráněné objekty.

4.11.4 Organizační opatření

Dle provedené kategorizace dat se provádí přiřazení uživatelů do skupin, které reprezentují práva cílového objektu. Všichni pracovníci by měli mít přístup k takovým objektům/aplikacím, které potřebují pro svou práci a které vyplývají z jejich kompetence. O nutnosti přístupu jednotlivých pracovníku rozhodují jejich řídicí pracovníci.

5 VLASTNÍ NÁVRH ŘEŠENÍ

5.1 Bezpečnostní cíle organizace

Společnost nemá jasné představy o bezpečnostních cílech, proto navrhuji podle doporučení literatury [9] následující cíl:

Eliminovat přímé a nepřímé ztráty, způsobené zneužitím, poškozením, zničením, nebo nedostupností informace. Vytvoření uceleného, nákladově optimalizovatelného a efektivně fungujícího procesu řízení bezpečnosti informací.

5.2 Bezpečnostní struktura organizace

Tabulka 2: Návrh bezpečnostní struktury organizace (Zdroj: Vyrobeno pro potřeby BP)

Funkce	Členové
Řídící výbor bezpečnosti	Jednatel a výkonný ředitel
Fórum bezpečnosti	Vedouci obchodu, Vedouci technologie, Vedoucí výstavby, Výkonný ředitel,Vedoucí IT
Bezpečnostní manager	Vedoucí IT
Bezpečnostní auditor	Jednatel, Vedoucí IT
Bezpečnostní správce	Systemový Administrátor

5.3 Analýza aktiv

Tabulka 3: Návrh analýzy informačních aktiv (Zdroj:Vyrobeno pro účely BP)

Typ aktiva	Název	Hodnota pro společnost	Důležitost (1-5)	Vlastník
Informační aktiva	Ekonomické informace	300 000 Kč	5	Účtárna
	Technická dokumentace	3 000 000 Kč	5	Projekce
	Fotogalerie základních stan	1 500 000 Kč	5	Technlogie
	Emailová komunikace	50 000 Kč	3	IT
	Archív	100 000 Kč	4	Projekce
	Smlouvy a dokumenty výstavby	10 000 000 Kč	5	Obchod
Programová	Stormware Pohoda	30 000 Kč	5	Účtárna
	Dispatcher	27 000 Kč	3	Doprava
	TachoScan	35 000 Kč	2	Doprava
	RTS	20 000 Kč	3	Obchod
	Interni IS	60 000 Kč	3	Technlogie
	Esxi	45 000 Kč	5	IT
	Operační systémy	340 000 Kč	3	IT
Fyzická aktiva	Dell Workstation	300 000 Kč	5	IT
	Dell Notebook	150 000 Kč	4	IT
	Serverovna	100 000 Kč	5	IT
	Racky	40 000 Kč	4	IT
	Dell Servery	450 000 Kč	5	IT
	Dell Storage MD 3000	120 000 Kč	5	IT
	Paskove mechaniky	18 000 Kč	4	IT
	NAS	5 000 Kč	3	IT
	Switche	180 000 Kč	5	IT
	Routery	10 000 Kč	5	IT
Služby	Připojení k síti Internet	7 000 Kč	5	IT

5.4 Ocenění aktiv

Návrh ocenění aktiv je součástí předchozí kapitoly. Zde je pro názornost uveden detailní výpočet pořizovací ceny některých vybraných aktiv.

Tabulka 4: Návrh výpočtu pořizovací ceny datových aktiv (Zdroj:Vyrobeno pro potřeby BP)

Fotogalerie základních stanic	
Počet základních stanic	2000
Průměrná doba cesty k základní stanici	3
Náklad na hodinu zaměstance	200 Kč
Prumerna vzdálenost Stanice	30
Náklad na 1 Km/cesty	5 Kč
Cena fotodokumentace jedné stanice	750 Kč
Celkem pořizovací cena	**1 500 000 Kč**

Technická dokumentace	
Počet stanic	2000
Průměrný naklad na hodinu projektanta	250 Kč
Průměrna doba vytvoření výkresu (hodiny)	2
Náklad na hodinu asistentky	100 Kč
Průměrná doba kompletace dokumentace(hodiny)	10
Hodnota jednoho výkresu	1 500 Kč
Celkem pořizovací cena	**3 000 000 Kč**

5.5 Klasifikace informací

Tabulka 5: Návrh klasifikace informací (Zdroj: Vyrobeno pro potřeby BP)

Skupiny informačních aktiv	Správce	Uživatel	Vlastník
Ekonomické informace	IT	Vedení	Účtárna
Technická dokumentace	IT	Technologie, Výroba, Vedení,Geodeti,Doprava	Projekce
Fotogalerie základních stanic	IT	Projekce, Výroba, Vedení,Geodeti,Doprava	Technologie
Emailová komunikace	IT	Vedení	IT
Archív	IT	Vedení, Technologie, Geodeti	Projekce
Smlouvy a dokumenty výstavby	IT	Vedení	Obchod

5.6 Analýza rizik

Komplexní zpracování analýzy rizik vyžaduje speciální metodiky a nástroje, které jsou popsány v teoretické části této práce. Vzhledem k jejich ceně a nedostupnosti navrhuji řešení od společnosti Microsoft MSAT, které reprezentuje neformální metodu analýzy rizik a je poskytováno zdarma. Detailní výstup programu MSAT je k dispozici v příloze č. 1 a 2.

Seznam rizik týkajících se ochrany dat

- R1 – Absence antivirové ochrany stanic a serveru.
  Míra rizika: **Vysoká**
- R2 – Absence metod zálohování a obnovy.
  Míra rizika: **Vysoká**
- R3 – Absence podmíněného přístupu k citlivým datům.
  Míra rizika: **Vysoká**
- R4 – Absence klasifikace dat.
  Míra rizika: **Vysoká**

Další vybraná rizika

- R5 – Riziko nesystematické řízení bezpečnosti.
  Míra rizika: **Vysoká**
- R6 – Riziko nevymahatelnosti odpovědnosti za škody.
  Míra rizika: **Nízká**
- R7 – Riziko z důvodu absence bezpečnostní politiky.
  Míra rizika: **Střední**
- R8 – Absence Update a Patch Managementu.
  Míra rizika: **Vysoká**
- R9 – Nedostatečné povědomím uživatelů o bezpečnosti.
  Míra rizika: **Vysoká**

Součásti této práce jsou pouze opatření týkající se specifické skupiny ochrany dat, nicméně pro komplexní pojetí informační bezpečnosti je nutné eliminovat všechna rizika a dále postupovat dle zmiňovaných postupů řešení informační bezpečnosti.

5.7 Návrh protiopatření vybraných rizik

5.7.1 Návrh řízení přístupu

Výsledek analýzy současného stavu přístupu datovým zdrojům

Tabulka 6: Analýza současného přístupu k datovým zdrojům (Zdroj:Vyrobeno pro potřeby BP)

Datové zdroje	Původní stav přístupu	Navrhovaný stav
Ekonomické informace	Volný - Čtení/Zápis	Role1: Čtení, Role2:Čtení/Zápis
Technická dokumentace	Částečný - Čtení/Zápis	Role3: Čtení, Role4:Čtení/Zápis
Fotogalerie základních stanic	Částečný - Čtení	Role5: Čtení, Role6:Čtení/Zápis
Emailová komunikace	Žádný	Role7: Čtení, Role8:Čtení/Zápis
Archiv	Částečný - Čtení/Zápis	Role9: Čtení, Role10:Čtení/Zápis
Smlouvy a dokumenty výstavby	Částečný - Čtení/Zápis	Role11: Čtení, Role12:Čtení/Zápis

Návrh řešení přístupu datových zdrojů

Tabulka 7: Přiřazení skupin k datovým zdrojům (Zdroj:Vyrobeno pro potřeby BP)

Název skupiny	Datový zdroj
Res_Ucto_Read	Ekonomické informace
Res_Ucto_Write	Ekonomické informace
Res_Technologie_Read	Technická dokumentace
Res_Technologie_Write	Technická dokumentace
Res_Foto_Read	Fotogalerie základních stanic
Res_Foto_Write	Fotogalerie základních stanic
Res_Mail_Read	Emailová komunikace
Res_Mail_Write	Emailová komunikace
Res_Dokumentace_Read	Smlouvy a dokumenty výstavby
Res_Dokumentace_Write	Smlouvy a dokumenty výstavby
Res_Archive_Read	Archiv
Res_Archive_Write	Archiv

Návrh přiřazení skupin k organizační struktuře společnosti

Tabulka 8: Přiřazení skupin k organizační struktuře společnosti (Zdroj vyrobeno pro potřeby BP)

Název skupiny	Uživatelé
Res_Ucto_Read	Ředitel,Asistenti ředitele
Res_Ucto_Write	Účtárna
Res_Technologie_Read	Výroba, Doprava
Res_Technologie_Write	Technologové,Projektanti, Geodeti
Res_Foto_Read	Projektanti, Geodeti,Reditel,Výroba, Doprava
Res_Foto_Write	Technologie
Res_Mail_Read	Ředitel
Res_Mail_Write	IT
Res_Dokumentace_Read	Obchod
Res_Dokumentace_Write	Ředitel,Asistenti ředitele
Res_Archive_Read	Ředitel,Asistenti ředitele, Technologie, Geodeti
Res_Archive_Write	Projektanti

Výsledek současného stavu přístupu k aplikacím

Tabulka 9: Analýza současného stavu přístupu k aplikacím (Zdroj:Vyrobeno pro potřeby BP)

Aplikace	Původní stav přístupu	Navrhovaný stav
Stormware Pohoda	Řízený	Řízený
Dispatcher	Volný	Řízený
Dochazka	Volný	Řízený
Tachoscan	Řízený	Řízený
RTS	Volný	Řízený
Interni IS Servisní zakázky	Volný	Řízený

Návrh přiřazení skupin aplikací k organizační struktuře společnosti

Tabulka 10: Přiřazení skupin aplikací k organizační struktuře společnosti (Zdroj: Vyrobeno pro potřeby BP)

Název skupiny	Aplikace	Uživatelé
Acn_pohoda	Stormware Pohoda	Ředitel,Asistent ředitele,Účtárna
Acn_dispatcher	Dispatcher	Ředitel,Asistent ředitele,Doprava
Acn_dochazka	Dochazka	Ředitel,Asistent ředitele,Vedoucí oddělení, Účtárna
Acn_Tachoscan	Tachoscan	Ředitel,Asistent ředitele,Doprava
Acn_RTS	RTS	Ředitel,Asistent ředitele,Obchod
Acn_Servis	Interni IS Servisní zakázky	Ředitel,Asistent ředitele,Technologie

Poznámky k implementaci:

Podobné schéma přístupu k datům lze libovolně rozšiřovat při dodržení bezpečnostních kriterií, tj. každý by měl mít přístup pouze tam, kde to vyžaduje jeho pracovní zařazení.

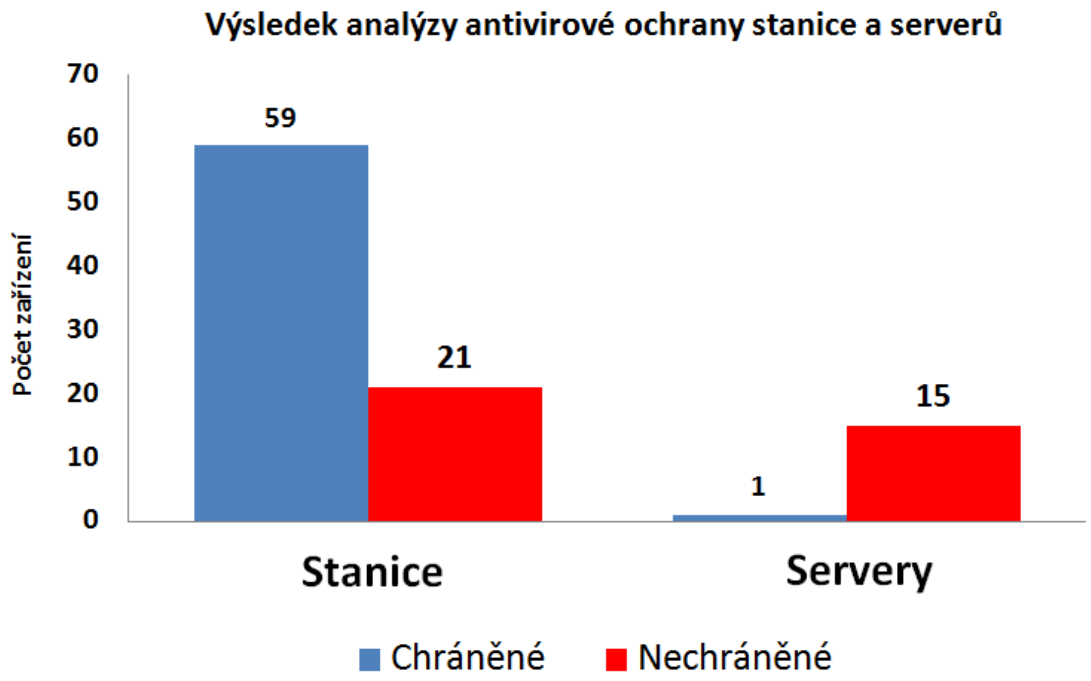
Cena řešení:

Rovná se nákladu IT pracovníků po dobu implementace, kterou odhaduji na 10 hodin. Při nákladu 500 Kč/hodina na oba pracovníky, je to 5000 Kč.

5.7.2 Návrh antivirového řešení

Výsledek analýzy současného stavu

Obrázek níže shrnuje výsledek průzkumu antivirové ochrany společnosti.



Obrázek 11: Výsledek analýzy antivirové ochrany stanic a serverů (Zdroj: Vyrobeno pro potřeby BP)

Návrh řešení

Na základě analýzy společnosti navrhuji antivirové řešení od společnosti Eset. Tato společnost je dlouhodobě hodnocena jako vydavatel spolehlivých bezpečnostních řešení. Mezi zákazníky této společnosti patří např. Fakulta Podnikatelská VUT v Brně. Výhodou je také vysoká úspěšnost v odhalování virových infiltrací. Neposledním důvodem je cena tohoto řešení.

Výběr produktů

Na základě složení infrastruktury společnosti doporučuji následující produkty firmy ESET:

Stanice: ESET Smart Security 4 Business Edition
File servery a Terminal Servery: Eset for File Servers and Terminal Servers
Produkčni servery: ESET Smart Security 4Business Edition
Centrální správa: ESET Remote Administrator 4.0

Poznámky k implementaci

Doporučuji, aby přiřazený IT pracovník sledoval aktuální verze antiviru, nejen aktualizace datových souborů, ale i verze programů - skenovací jádro a také včas implementoval nové verze. Součástí nastavení aktualizace notebooků musí být možnost aktualizace přes internet v případě nedostupnosti interního aktualizačního serveru.

Doporučuji také proškolení uživatelů o potenciálních zdrojích nákazy, tj. např. stahování neznámých souborů z internetu nebo otevírání podezřelých příloh pošty apod. Toto vzdělávání by mělo být povinné jak v rámci vstupního zaškolení, tak i při opakovaném přeškolení zaměstnanců.

Cena řešení

Tabulka 11: Kalkulace řešení od firmy ESET (Zdroj: Vyrobeno pro potřeby BP)

Počet	Produkt	Cena za kus bez DPH	Celkem bez DPH
1	ESET NOD32 File Security na Linux	3 456 Kč	**3 456 Kč**
1	ESET NOD32 Windows File Server	3 456 Kč	**3 456 Kč**
13	ESET Smart Security 4 Business Edition Servery	749 Kč	**9 737 Kč**
1	Upgrade na ESET Smart Security 4 Business Edition	489 Kč	**489 Kč**
59	Upgrade na ESET Smart Security 4 Business Edition	489 Kč	**28 851 Kč**
21	ESET Smart Security 4 Business Edition Stanice	749 Kč	**15 729 Kč**
1	ESET Remote Administrator 4	0 Kč	**0 Kč**
		Celkem	61 718 Kč

Cena nákladu IT pracovníků po dobu implementace, kterou odhaduji na 30 hodin, je při nákladu 500 Kč/hodina na oba pracovníky, 15000 Kč.

5.7.3 Návrh zálohovacího mechanizmu

Výsledek analýzy současného stavu

Společnost neřešila danou problematiku.

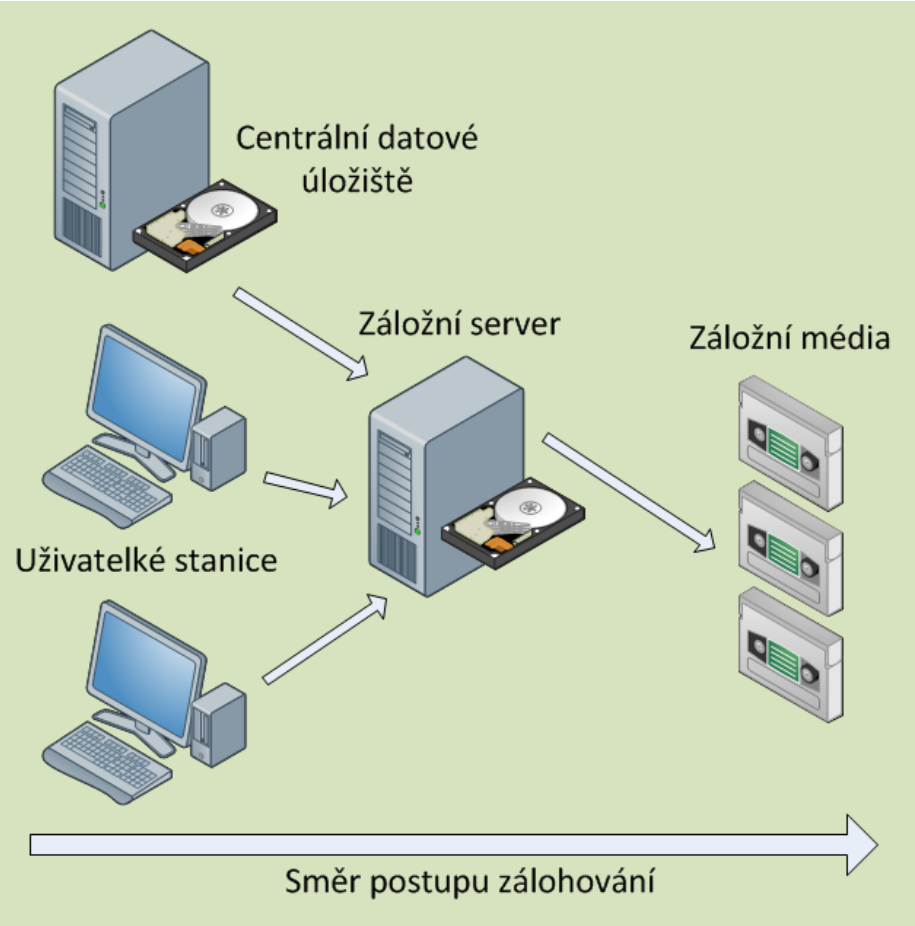
Návrh řešení

Analýza aktiv ukázala, která data se mají chránit, proto navrhuji tuto skupinu dat jako součást záloh.

- Ekonomické informace
- Technická dokumentace
- Emailová komunikace
- Fotogalerie základních stanic
- Smlouvy a dokumenty výstavby
- Archiv

Vzhledem ke struktuře zálohovaných dat navrhuji blokovou zálohu dat. Společnost požaduje rychlou obnovu dat a tu upřednostňuje před cenou navrhovaného řešení. Z tohoto důvodu navrhuji schéma D2D2T a jako software pro zálohování IBM Tivoli Storage Manager FastBack. Další požadavky jsou shrnuty v návrhu politiky zálohování, viz. příloha č. 4.

Zobrazení navrhovaného schématu zálohování



Obrázek 12: Směr postupu zálohování (Zdroj: Vyrobeno pro potřeby BP)

Poznámky k implementaci

Proces zálohování by měl být upravován dle aktuálních potřeb společnosti.

Cena řešení

Cena řešení pro zálohu 1 datového Serveru a archivaci na pásku je 55 000 Kč bez DPH Cena nákladu IT pracovníků po dobu implementace, kterou odhaduji na 40 hodin, je při nákladu 500 Kč/hodina na oba pracovníky, 20 000 Kč.

6 ZHODNOCENÍ

6.1 Srovnání aktuálního stavu s navrhovaným

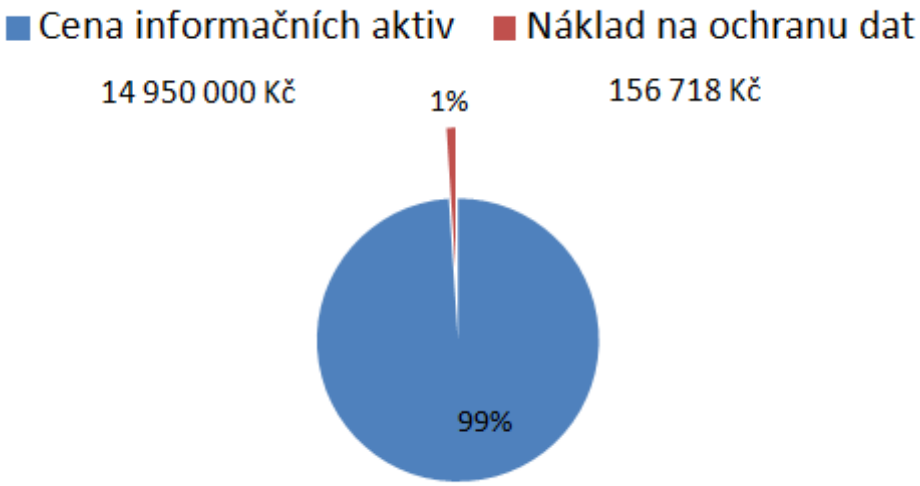
Tabulka 12: Srovnání aktuálního stavu s navrhovaným (Zdroj: Vyrobeno pro potřeby BP)

Metody ochrany dat	Původní stav	Navrhovaný stav
Zálohování	Žádné	Blokové ve schématu D2D2T
Antivirová ochrana	Částečná	Chráněny stanice i servery
Řízení přístupu k datům	Nahodilé, nesystematické	Systematické, přístup definován dle rolí

Dále byla provedena klasifikace informací a také identifikace a ocenění aktiv společnosti.

6.2 Ekonomické zhodnocení navrhovaného řešení

6.2.1 Porovnání nákladů a celkové ceny



Obrázek 13: Porovnání nákladů a celkové ceny řešení (Zdroj: Vyrobeno pro potřeby BP)

6.2.2 Struktura nákladů

Náklad na ochranu dat byl vypočten jako součet těchto položek:

- Náklad na zálohování: 55 000 Kč
- Náklad na antivirus: 61 718 Kč
- Cena implementace IT pracovníky: 40 000 Kč

Doba implementace byla odhadována na 80 hodin.

6.2.3 Zhodnocení

Cena ochrany dat je tedy 1% z celkové hodnoty chráněných aktiv. Pro společnost je to významný ukazatel pro investice do implementace bezpečnosti. Tento propočet ale není konečný, neboť zde nejsou zohledněny další oblasti bezpečnosti (fyzická, organizační, technická a další).

7 ZÁVĚR

Rozbor stávajících metod ochrany společnosti ukázal, že byly tendence chránit data nevýznamné důležitosti, ale data důležitá byla opomenuta. Poukázal také na chybějící bezpečnostní mechanizmy. Společnost tedy problematiku ochrany dat neřešila, předpokládala, že je vše v pořádku a možné bezpečnostní incidenty zůstaly bez povšimnutí.

Byly odhaleny oblasti, které by mohly mít za následek ztrátu důvěryhodnosti, integrity, nedostupnosti dat. Na základě těchto poznatků byly navrženy vhodné metody ochrany. Jedná se zejména o řízení přístupu, systém zálohování dat a komplexní antivirové ochrany. Součástí návrhu je také ekonomická analýza, která porovnává celkovou cenu navrhovaného řešení s cenou chráněných aktiv.

Implementací technických doporučení však ochrana dat nekončí, ale začíná, je třeba zohlednit další zmiňované oblasti jako např. vypracování bezpečnostní politiky, provádění bezpečnostních školení zaměstnanců atd.

Tato bakalářská práce zahrnuje pouze omezený pohled na problematiku vzhledem k jejímu širokému spektru pokrytí, které je závislé na typu podniku, struktuře aktiv, infrastruktuře a bezpečnostních cílech podniku.

Součástí práce jsou také odkazy na další vhodné zdroje literatury, které by mohly být využity k analýze a návrhu ochrany dat dalších společností.

Doporučená opatření by mohla být použita jako podklad pro diplomovou práci na podobné téma, případně téma týkající se bezpečnostní politiky organizace.

SEZNAM POUŽITÉ LITERATURY

Knihy a tištěné materiály

[1] ARNASON, Sigurjon Thor, WILLETT, Keith D. *How to Achive 27001 Certificaiton : An Example of Applied Comliance Management*. London : Auerbach Publications, 2008. 348 s. ISBN 978-0-8493-3648-5.

[2] CALDER, Alan, WATKINS, Steve. *IT GOVERNANCE : A Manager's Guide to Data Security and ISO 27001/ISO27002*. London : Kogan Page, 2008. 372 s. ISBN 978-0-7494-5271-1.

[3] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha : Grada Publishing, spol. s r.o., 1998. 286 s. ISBN 80-7169-479-7.

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, a.s., 2004. 190 s. ISBN 80-251-0106-1.

[5] HANÁČEK, Petr; STAUDEK, Jan. *Bezpečnost informační systémů*. Praha : Úřad pro státní informační systém, 2000. 128 s. ISBN 80-238-5400-3.

[6] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006. 200 s. ISBN 80-7318-456-7.

[7] POŽÁR, Josef. *Informační bezpečnost*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk,s,r.o., 2005. 311 s. ISBN 80-86898-38-5.

[8] POŽÁR, Josef. *Manažerská Informatika II*. Praha : Vydavatelství PA ČR, 2006. 222 s. ISBN 80-7251-232-3.

[9] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha : Vydavatelství PA ČR, 2007. 219 s. ISBN 978-80-7251-250-8.

Elektronické zdroje

[10] *ESET* [online]. 2010 [cit. 2010-05-30]. Srovnání antivirů a bezpečnostních řešení. Dostupné z WWW: <http://www.eset.cz/srovnani-antiviru>.

[11] MLÝNEK, Jaroslav. *Fp.vslib.cz* [online]. 2007 [cit. 2010-05-25]. Zabezpečení obchodních informací. Dostupné z WWW: <http://www.fp.vslib.cz/kmd/lide/mlynek/ZOI/ke%20zkousce/ZOI-StudMater07-08.pdf>.

[12] PŘIBYL, Tomáš. *ICT Security* [online]. 2010 [cit. 2010-05-27]. Chránit lze jen to, v čem máme pořádek. Dostupné z WWW: <http://www.ictsecurity.cz/odborne-clanky/chranit-lze-jen-to-v-cem-mame-poradek.html>.

[13] *U.S. Data Trust* [online]. 2002 [cit. 2010-05-24]. Safeguarding Your Critical Data: A Practical Guide to Data Protection and Recovery. Dostupné z WWW: <http://www.usdatatrust.com/resources/Data_Protection_White_Paper.pdf>.

[14] WARTELL, David . *Backup Software Technology* [online]. 10. 12. 2008 [cit. 2010-05-25]. Backup Software Technology Whitepaper. Dostupné z WWW: <http://wiki.r1soft.com/pages/doexportpage.action?pageId=5439599&type=TYPE_PDF>.

Normy a Zákony

[15] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2006. 36 s. ISSN 8-598563-765334.

[16] ČSN ISO/IEC 17799. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací*. Praha: Český normalizační institut, 2006. 102 s. ISSN 8-590963-759012.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

PŘÍLOHY

Příloha č. 1: Výstup z programu MSAT – celkové shrnutí

Příloha č. 2: Rozpis doporučení týkající se datové bezpečnosti

Příloha č. 3: Položené otázky a odpovědi týkající se provozu IT.

Příloha č. 4: Návrh zálohovací politiky

Příloha č. 1: Výstup z programu MSAT – celkové shrnutí

Legenda: ● Splňuje požadavky ● Nutné zlepšení ● Nedostatečné

Infrastructure	●
Perimeter Defense	●
Firewall Rules and Filters	●
Anti-virus	●
Anti-virus - Desktops	●
Anti-virus - Servers	●
Remote Access	●
Segmentation	●
Intrusion-Detection System (IDS)	●
Wireless	●
Authentication	●
Administrative Users	●
Internal Users	●
Remote-Access Users	●
Password Policies	●
Password Policies - Administrator Account	●
Password Policies - User Account	●
Password Policies - Remote-Access Account	●
Inactive Accounts	●
Management and Monitoring	●
Incident Reporting & Response	●
Secure Build	●
Physical Security	●
Applications	●
Deployment and Use	●
Load-Balancing	●
Clustering	●
Application & Data Recovery	●
Third-party independent software vendor (ISV)	●
Internally Developed	●
Vulnerabilities	●
Application Design	●
Authentication	●
Password Policies	●
Authorization & Access Control	●
Logging	●
Input Validation	●
Software Security Development Methodologies	●
Data Storage & Communications	●
Encryption	●
Encryption - Algorithm	●

Operations	●
Environment	●
Management Host	●
Management Host - Servers	●
Management Host - Network Devices	●
Security Policy	●
Data Classification	●
Data Disposal	●
Protocols & Services	●
Acceptable Use	●
User Account Management	●
Governance	●
Security Policies	●
Patch & Update Management	●
Network Documentation	●
Application Data Flow	●
Patch Management	●
Change Management and Configuration	●
Backup and Recovery	●
Log Files	●
Disaster Recovery & Business Resumption Planning	●
Backup	●
Backup Media	●
Backup & Restore	●
People	●
Requirements & Assessments	●
Security Requirements	●
Security Assessments	●
Policy & Procedures	●
Background Checks	●
Human Resources Policy	●
Third-Party Relationships	●
Training & Awareness	●
Security Awareness	●
Security Training	●

Příloha č. 2: Rozpis doporučení týkající se datové bezpečnosti:

Subcategory	Best Practices	
Anti-virus	Deploy anti-virus solutions throughout the environment on both the server and desktop levels. Deploy specialized anti-virus solutions for specific tasks such as file server scanners, content screening tools, and data upload and download scanners. Configure anti-virus solutions to scan for viruses both entering and leaving the environment. Anti-virus solutions should be implemented first on critical file servers and then extended to mail, database, and Web servers. For desktops and laptops an anti-virus solution should be included in the default build environment. If you are using Microsoft Exchange, use the additional anti-virus and content filtering-capabilities it offers at the mailbox level.	
	Findings	**Recommendations**
Anti-virus	You have indicated that perimeter hosts do not have anti-virus software installed.	Anti-virus software should be installed on all machines in the corporate environment.
Subcategory	**Best Practices**	
Anti-virus - Desktops		
	Findings	**Recommendations**
Anti-virus - Desktops	Your answer indicates that anti-virus solutions have been deployed at the desktop level.	Continue the practice. Implement a policy that requires users to regularly update virus signatures. Consider adding the anti-virus client in the default workstation build environment.
	Findings	**Recommendations**
Anti-virus - Servers	You indicated that anti-virus solutions have not been deployed at the server level.	Consider deploying an anti-virus solution to critical file servers initially and then to e-mail, database, and web servers. If you are using Microsoft Exchange, consider using the additional anti-virus and content-filtering capabilities at the mailbox level.

Subcategory	Best Practices
Authorization & Access Control	Applications should implement an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. Role-based access controls should be enforced at the database level as well as at the application interface. This will protect the database in the event that the client application is exploited. Authorization checks should require prior successful authentication to have occurred. All attempts to obtain access without proper authorization should be logged. Conduct regular testing of key applications that process sensitive data and of the interfaces available to users from the Internet. Include both "black box" and "informed" testing against the application. Determine if users can gain access to data from other accounts.

	Findings	Recommendations
Authorization & Access Control	Your response indicates that key applications restrict access to sensitive data and functionality based on privileges assigned to the account.	Consider conducting focused application testing on key applications that process sensitive data and on the interfaces available to users from the Internet. Include both 'black box' and 'informed' testing against the application and test for privilege escalation.

Security Policy	
Subcategory	**Best Practices**
Data Classification	Continue to implement data classification with corresponding protection guidelines.
Data Classification	Define a corporate data classification scheme and provide all staff with appropriate training and guidance regarding data classification. Define useable handling and protection requirements corresponding to data classification levels.
Data Classification	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.

Data Classification	It is important to have a data classification scheme with corresponding data protection guidelines. Insufficient information "classification" and segregation can allow staff, business partners, or the public access to information that is sensitive or that they do not have a "need-to-know." This could lead to loss of brand image or corporate embarrassment owing to unauthorized disclosure of sensitive information. Scarce resources used to secure information may also be misallocated without proper information classification. Without the staff knowing what company sensitive information is and how to protect this data, there is a high likelihood that this information may be exposed to unauthorized persons.	
	Findings	**Recommendations**
Data Classification	You have indicated that you do not know the answer to this question	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.
Subcategory	**Best Practices**	
Data Disposal	Continue to implement data disposal processes.	
Data Disposal	Define and implement procedures for the management and disposal of information in both hard copy and electronic form, such as that contained on floppy disks and harddrives.	
Data Disposal	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.	
Data Disposal	Formal procedures should exist so that all users know the proper practices for disposing of electronic and hardcopy information. By not providing guidance and processes for securely destroying information, the confidentiality of information could be compromised.	
	Findings	**Recommendations**
Data Disposal	You have indicated that you do not know the answer to this question	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.

Subcategory	**Best Practices**
Disaster Recovery & Business Resumption Planning	Continue to maintain and test disaster recovery / business resumption plans.

Disaster Recovery & Business Resumption Planning	Require disaster recovery plans to be developed, documented, implemented, and subjected to periodic reviews, tests, and updates. Develop Business Continuity Plans that include staff, locations, as well as systems and other technology issues.
Disaster Recovery & Business Resumption Planning	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.
Disaster Recovery & Business Resumption Planning	Disaster Recovery and Business Resumption plans should be well documented and up-to-date, to ensure recovery in an acceptable timeframe. Plans (including restore from backup for applications) should be regularly tested to validate correctness and completeness. Business Continuity Plans should focus on the entire environment; physical, technological, and staff.

	Findings	**Recommendations**
Disaster Recovery & Business Resumption Planning	You have indicated that you do not know the answer to this question	Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information.

Subcategory	**Best Practices**
Backup	Full backups should be performed at regular intervals. If feasible, partial intermediary backups should be made between full backups. The backup strategy should address the worst-case scenario of a complete system and application restore. For critical applications, the restore process should result in a fully functioning application in minimal time.

	Findings	**Recommendations**
Backup	Your answer indicates that critical assets are not being backed up on a regular basis.	Identify all critical assets based on business needs, and work on implementing a backup mechanism for each of the critical assets based on listed best practices.

Subcategory	**Best Practices**
Backup Media	Detailed policies should exist to govern the storage and handling of backup media. These policies should address issues such as: Onsite/OffsiteStorage MediaRotation Security Controls Personnel Access Controls

	Removable backup media should be stored in locked, fire-proof cabinets and only authorized personnel should have access to these cabinets. Offsite storage locations should be used to offer greater recoverability in the event of disaster.
Subcategory	**Best Practices**
Backup & Restore	Backup and restore procedures should be tested regularly to identify faulty media and improve the chance of a successful restore in the event of an outage. Detailed procedures for restoring different systems, including applications, should be well-documented. Audit all the backup and restore documents to ensure all the critical systems necessary for business continuity are covered.

Příloha č. 3: Položené otázky a odpovědi týkající se provozu IT.

Operations	
Does the company manage the environment itself, or outsource?	The company manages the environment
Does the organization use dedicated management hosts for secure administration of systems and devices within the environment?	No
Are separate login accounts used for normal activity vs. administrative/management activity?	No
Does the organization grant users administrative access to their workstations and/or laptops?	No
Is the firewall tested regularly to ensure it performs as expected?	No
Does your organization maintain Disaster Recovery and Business Resumption Plans?	No
Does a model exist for assigning criticality levels to each component of the computing environment?	No
Do policies exist to govern the computing environment?	No
Does a documented process exist for host builds? If yes, which types? (For what host types does a documented build process exist?)	Workstations and laptops
Do documented guidelines exist that govern which protocols and services are allowed on the corporate network? Select the option that applies.	Guidelines exist, but they are not documented
Does your organization have a formal, well-documented process for the disposal of data on electronic media and hardcopy form?	No
Does your organization have a data classification scheme with associated data protection guidelines?	No
Does a change and configuration management process exist?	No

Does an established patch and update policy and process exist?	No
Does an established policy exist to govern the updating of signature-based detection products?	Anti-virus
Do accurate logical diagrams and supporting configuration documentation exist for the network infrastructure and hosts?	No
Do accurate application architecture and data flow diagrams exist for key applications?	No
Is logging enabled in the environment to record events on hosts and devices?	No
Is critical and sensitive data backed up on a regular basis?	No

Příloha č. 4: Návrh zálohovací politiky

Zálohovací politika firmy Svoboda a Syn s.r.o.

Historie revizí

Číslo revize	Datum	Důvod revize	Revidoval
1.0	31. 5. 2010	První verze	Miroslav Koutný

Cíl a rozsah politiky

Cílem politiky je:

- Zabránit ztrátě dat, v případě náhodného smazání, poškození nebo selhání systému;
- Zabezpečit informační základnu společnosti Svoboda a Syn s.r.o.;
- Zajistit včasné obnovení dat;
- Zodpovědně řídit proces zálohování a obnovy dat.

Politika se vztahuje na:

- Všechny servery a datové pole společnosti Svoboda a syn s.r.o.

POPIS rolí

Management

- Zajistí fyzickou bezpečnost serverovny;
- Úschovu archivních medii do trezoru;
- Zajišťuje pravidelnou úschovu záložních medii mimo společnost v pevně stanovených intervalech.

Administrátor

- Zabezpečuje proces zálohování a obnovy;
- Ověřuje stav zálohy a v případě potřeby řeší problémy.

Ostatní zaměstnanci

- Ukládají data na síťové disky, tyto data jsou zálohovány;
- V případě uložených dat na jiných místech než síťových discích jsou zodpovědni za zálohu či obnovu těchto dat.

Popis politiky

Záloha dat

Data uložena na centrálním datovém úložišti budou zálohována dle následujícího schématu:

- Online 24x7 zálohou všech změn diskových sektorů na záložní disk zálohovacího serveru.
- Revize změn jednotlivých souborů bude ukládána 5 revizí zpetně.
- V nočních hodinách Po-Pá bude probíhat inkrementální záloha na páskové medium.
- O víkendu bude proveden Full Backup na páskové medium
- Následující pondělí budou tyto záložní media odvezeny mimo společnost Svoboda a Syn s.r.o.
- Systémové a aplikační disky virtuálních serveru budou uloženy ke konci každého měsíce na externí NAS pole.
- NAS je jednou za 3 měsíce přepsáno a uloženo na páskové medium. To je pak uloženo mimo areál společnost Svoboda a Syn.

Obnova dat

Požadavek na obnovu se vyřizuje dle priorit. Rozhoduje požadavek skupiny nad požadavkem jednotlivce.

Audit/Testování

- V pravidelném intervalu 6 měsíců dochází k auditu této bezpečnostní směrnice. Je prověřeno, zda stále odpovídá potřebám organizace, a případně potřeby bude provedena její změna. Změna bude zohledněna v seznamu revizi.
- Každý měsíc bude proveden testovací obnovení dat ze záložních medií. V případě neúspěšného pokusu obnovy, bude provedeno nalezení a odstranění příčiny.

Přiřazení odpovědností

Zálohování a obnova dat:	Martin Černý
Zálohovaní a obnova serveru:	Miroslav Koutný
Verifikace a monitorováni:	Ing. Luděk Batelka, Bc. Pavel Novák

Sankce

Nedodržení těchto postupů bude považováno za hrubé porušení pracovní kázně a může vést i k ukončení pracovního poměru zaměstnance.